



Installationsbedingungen

SERVER

Voraussetzung für den Server ist ein Betriebssystem mit vorhandener Microsoft® SQL-Datenbank oder der Möglichkeit eine Microsoft® SQL-Datenbank zu installieren. Standardmäßig wird MSDE SP4 in einem TCP/IP-Umfeld installiert.

Mindestanforderungen:

Pentium III 1000 MHz 1024 MB RAM
20 GB freie Festplattenkapazität ¹⁾
100 MBit LAN
Windows 2000 Professional SP4
Windows 2003 Server
Windows XP Professional

Ideale Anforderungen:

P4 3 GHz 1024 MB RAM
60 GB freie Festplattenkapazität

100 MBit LAN
Windows Server 2003

Für alle Betriebssysteme müssen die aktuellen Updates und Patches von Microsoft installiert sein

Um die Update-Prozedur störungsfrei durchführen zu können, braucht der Client Administrator-Rechte lokal auf dem PC.

BIZS-Freigabe am Server:

Auf dem Server wird eine Server-Freigabe (SHARE) für BIZS\$ erstellt. Alle Benutzer sollten hier entsprechend Zugriffe vom Betriebssystem aus haben.

Zu beachten bei XP-Professional und Vista:

Die Firewall muss auf dem Server mit einem Port TCP 1433 und UDP 1434 erweitert werden.

CLIENT (Arbeitsplatz)

Mindestanforderungen:

Pentium III 1000 MHz 512 MB RAM
20 GB freie Festplattenkapazität ¹⁾
100 MBit LAN

Windows 2000 Professional SP4
MDAC 2.81

Windows XP Professional

Windows VISTA Business

Bildschirmauflösung 1024 x 768

Für alle Betriebssysteme müssen die aktuellen Updates und Patches von Microsoft installiert sein

Ideale Anforderungen:

Pentium IV 2,8 GHz mit HAT 1024 MB
20 GB freie Festplattenkapazität ¹⁾
100 MBit LAN

Microsoft Windows XP Professional SP2

Microsoft Office 2003

Bildschirmauflösung 1024 x 768

Vorbereitung der Grundinstallation von BIZS vom Kunde vor der Installation von BIZS zu erledigen

Wir arbeiten mit .NET 2 und daher installieren Sie bitte die folgenden Programme, die Sie zuvor downloaden.

.NET Framework 2.0 von Microsoft:

www.bizs.de/bizs_down/dotnetfx.exe

www.bizs.de/bizs_down/vjredist.exe

Bitte installieren Sie nur auf dem Server:

www.bizs.de/bizs_down/WindowsInstaller-KB893803-v2-x86.exe

CTI-Vorbereitung

BIZS unterstützt CTI (Computer Telefonie). Bitte installieren Sie den TAPI Treiber (ab Version 2.1 aufwärts) an Ihrem PC. Wichtig: Die CTI ist nur dann nutzbar, wenn unter Systemsteuerung / Modem / CTI die Anschlüsse hier sichtbar sind. Weitere Informationen finden Sie im Administratorenhandbuch von BIZS.

Sicherung von Daten

Generell ist der Kunde selbst für die ordentliche Sicherung seiner Daten und die Daten von BIZS verantwortlich. Alle von BIZS benötigten Daten werden im Verzeichnis BIZS des Servers abgelegt. Eventuelle Datenbank-Dumps sind vom Kunden in gegebenen Zeitabständen zu prüfen.

Wichtig: BIZS verfügt über keine Papierkorb- oder Rückgängig-Funktion. Ein Wiederherstellen versehentlich gelöschter Daten ist nur über die Datensicherung möglich.

Datenübernahme aus bisher verwendeten Systemen:

Eine Übernahme der Adressdaten, von Artikeln und Leistungen erspart Ihnen viel Arbeit, Zeit und damit Geld und ermöglicht Ihnen den sofortigen Start mit BIZS.

Hierfür benötigen wir:
Ihre Adressdaten als Excel-Tabelle, andere Formate erfordern Rücksprache
Ihre Artikel- und Leistungsdaten als Excel-Tabelle, andere Formate erfordern Rücksprache

Beleganpassung:

Wir passen Ihnen Ihre Belege (Ausgangsrechnung, Auftrag, Gutschrift oder Angebot) an Ihr vorgedrucktes Briefpapier an oder wir integrieren Ihr Logo und Ihre Kontaktdaten auf dem Beleg. Eine Integration Ihres Briefpapiers als Wasserzeichen ist ebenfalls möglich.

Hierfür benötigen wir:
Ihr Logo oder Briefpapier als Datei in den Formaten .jpeg, .gif, oder .pdf
Einen Originalausdruck ihrer bisher verwendeten Belege
Eine detaillierte und genaue Beschreibung des Belegs mit allen erforderlichen Firmendaten (Bankverbindung, Ust-Nr, HRB, usw.).

Nutzung von BIZS

Internet-Update und Dokumentation

Folgende Internet-Services werden von BIZS zur Verfügung gestellt:

- INTERNET-Update: Kunde führt seine Updates selbst durch
- BUG-Report: Alle Fehler und Wünsche bzw. Anregungen werden in BIZS im Modul BUG-Report eingetragen. Diese Daten werden direkt im Internet-Server von BIZS gespeichert
- BIZS-Historie: Alle Änderungen und Neuerungen werden im Modul BIZS-Historie bereitgestellt.
- Video: alle Beschreibungen zu Vorgängen und Modulen werden als Video bereitgestellt.
- Handwerk: Leistungen und Artikel werden über den Internet-Server bereitgestellt.

Um diese Dienste nutzen zu können, müssen Sie Ihre Firewall wie folgt schalten

TCP/IP von innen nach aussen: Port 1433 und Port 1434

Wichtig: Firewall-Einstellungen für XP und andere Betriebssysteme

Konfiguration der Netzwerkeinstellungen und Einrichten der Firewall unter Windows XP SP2

Damit eine SQL Server -Instanz im Netzwerk erreichbar ist, müssen Sie die Netzwerkprotokolle konfigurieren und ggf. einschalten. Sollten Sie SQL Server Express auf einem Windows XP-System mit Service Pack 2 betreiben, und dieser Rechner nicht Teilnehmer einer Active Directory Domäne sein, müssen Sie obendrein die Firewall konfigurieren:

- Um die Netzwerkprotokolle einzurichten, starten Sie den SQL Configuration Manager aus dem Startmenü (Start/Alle Programme/Microsoft SQL Server 2005/Konfigurationstools/SQL Server Configuration Manager).
- Öffnen Sie in der linken Baumstruktur den Zweig SQL Server 2005-Netzwerkconfiguration, und klicken Sie auf Protokolle für 'SQLEXPRESS'.
- Öffnen Sie in der rechten Liste das Kontextmenü über dem Eintrag Named Pipes. Wählen Sie aus dem Kontextmenü den Eintrag Aktivieren.
- Öffnen Sie das Kontextmenü in der rechten Liste über dem Eintrag TCP/IP. Wählen Sie aus dem Kontextmenü den Eintrag Aktivieren.

Firewall-Einstellungen unter Windows XP SP2

Falls sich SQL Server auf einem Windows XP-SP2-Rechner befindet, der nicht zu einer Active Directory-Domäne gehört, schalten Sie die entsprechenden Ports für den SQL Server- bzw. SQL Browser-Dienst frei. Dazu wählen Sie aus der Systemsteuerung Windows Firewall.

- Aktivieren Sie in der Ausnahmenliste die Datei- und Druckerfreigabe, da nur so die Ansteuerung über Named Pipes funktionieren wird (Port 445). Dieser Port ist standardmäßig in der Ausnahmenliste vorhanden.
- Klicken Sie auf der Registerkarte Ausnahmen auf Port, und geben Sie den TCP Port 1433 frei. Dieser Port wird standardmäßig für die erste SQL Server-Instanz vergeben.

- Öffnen Sie zusätzlich den UDP-Port 1434, 1433 sowie UDP-Port 1434, um »von Außen« den SQL Server erreichen zu können. Öffnen Sie ebenfalls den Port für die Datei- und Druckerfreigabe, um über Named Pipes auf SQL-Server zugreifen zu können (Port 445, bereits in der Ausnahmenliste vorhanden).

Wenn Sie versuchen, von einem Remotecomputer aus eine Verbindung zu einer Instanz von Microsoft SQL Server 2005 herzustellen, kann eine Fehlermeldung angezeigt werden. Dieses Problem kann bei einem beliebigen Programm auftreten, das Sie zur Herstellung der Verbindung zu SQL Server verwenden. Beispielsweise wird folgende Fehlermeldung angezeigt, wenn Sie mit dem Dienstprogramm SQLCMD eine Verbindung zu SQL Server herstellen (sinngemäß):

Sqlcmd: Fehler: Microsoft SQL Native Client: Fehler beim Versuch, eine Verbindung zum Server herzustellen. Beim Herstellen einer Verbindung zu SQL Server 2005 kann der Fehler dadurch verursacht werden, dass die SQL Server-Standardinstellungen Remoteverbindungen nicht zulassen.

(An error has occurred while establishing a connection to the server. When connecting to SQL Server 2005, this failure may be caused by the fact that under the default settings SQL Server does not allow remote connections.)

Dieses Problem kann auftreten, wenn SQL Server 2005 nicht für das Annehmen von Remoteverbindungen konfiguriert ist. Standardmäßig lassen SQL Server 2005 Express Edition und SQL Server 2005 Developer Edition Remoteverbindungen nicht zu. Gehen Sie folgendermaßen vor, um SQL Server 2005 so zu konfigurieren, dass Remoteverbindungen zugelassen werden:

- Aktivieren Sie Remoteverbindungen auf der Instanz von SQL Server, zu der Sie eine Verbindung von einem Remotecomputer herstellen möchten.
- Aktivieren Sie den SQL Server-Browser-Dienst.
- Konfigurieren Sie die Firewall so, dass Netzwerkverkehr zugelassen wird, der mit SQL Server und dem SQL Server-Browser-Dienst zusammenhängt.

Dieser Artikel beschreibt die Vorgehensweise für die einzelnen Schritte.

Verwenden Sie das Oberflächen-Konfigurationstool in SQL Server 2005, um Remoteverbindungen für die Instanz von SQL Server 2005 zu ermöglichen und den SQL Server-Browser-Dienst zu aktivieren. Das Oberflächen-Konfigurationstool wird bei der Installation von SQL Server 2005 installiert.

Remoteverbindungen für SQL Server 2005 Express oder SQL Server 2005 Developer Edition ermöglichen

Sie müssen Remoteverbindungen für jede Instanz von SQL Server ermöglichen, zu der Sie eine Verbindung von einem Remotecomputer herstellen möchten. Gehen Sie hierzu folgendermaßen vor:

1. Klicken Sie auf **Start**, zeigen Sie auf **Programme**, auf **Microsoft SQL Server 2005**, auf **Konfigurationstools**, und klicken Sie anschließend auf **SQL Server-Oberflächenkonfiguration**.
2. Klicken Sie auf der Seite **SQL Server 2005-Oberflächenkonfiguration** auf **Oberflächenkonfiguration für Dienste und Verbindungen**.
3. Erweitern Sie **Datenbankmodul** auf der Seite **Oberflächenkonfiguration für Dienste und Verbindungen**, klicken Sie auf **Remoteverbindungen**, auf **Lokale Verbindungen und Remoteverbindungen**, klicken Sie auf das für Ihre Umgebung zu aktivierende Protokoll und anschließend auf **Übernehmen**.

Hinweis: Klicken Sie auf **OK**, wenn die folgende Meldung angezeigt wird:

Änderungen der Verbindungseinstellungen werden erst nach einem Neustart des Datenbankmoduldienstes wirksam.

4. Erweitern Sie **Datenbankmodul** auf der Seite **Oberflächenkonfiguration für Dienste und Verbindungen**, klicken Sie auf **Dienst**, auf **Beenden**, warten Sie, bis der Dienst MSSQLSERVER beendet wird, und klicken Sie anschließend auf **Start**, um den Dienst MSSQLSERVER neu zu starten.

SQL Server-Browser-Dienst aktivieren

Wenn Sie SQL Server 2005 mit einem Instanznamen ausführen und keine spezielle TCP/IP-Portnummer in Ihrer Verbindungszeichenfolge verwenden, müssen Sie den SQL Server-Browser-Dienst aktivieren, um Remoteverbindungen zu ermöglichen. SQL Server 2005 Express wird z. B. mit dem Standardinstanznamen *Computername\SQLEXPRESS* installiert. Sie müssen den SQL Server-Browser-Dienst nur einmal aktivieren, unabhängig von der Anzahl der Instanzen von SQL Server 2005, die Sie ausführen. Gehen Sie folgendermaßen vor, um den SQL Server-Browser-Dienst zu aktivieren.

Wichtig: Diese Schritte können zu einem erhöhten Sicherheitsrisiko führen. Diese Schritte können außerdem Ihren Computer oder Ihr Netzwerk anfälliger für Angriffe

durch böswillige Benutzer oder gefährliche Software, wie etwa Viren, machen. Microsoft empfiehlt, den in diesem Artikel beschriebenen Prozess zu verwenden, um den vorgesehenen Betrieb von Programmen zu ermöglichen oder um spezielle Programmfunktionen einzusetzen. Wir raten Ihnen jedoch, zunächst die Risiken der Verwendung dieses Prozesses für Ihre Umgebung abzuschätzen, bevor Sie die genannten Änderungen vornehmen. Wenn Sie sich entscheiden, diesen Prozess anzuwenden, führen Sie alle entsprechenden zusätzlichen Schritte durch, um Ihr System zu schützen. Sie sollten diesen Prozess nur anwenden, wenn dies wirklich erforderlich ist.

1. Klicken Sie auf **Start**, zeigen Sie auf **Programme**, auf **Microsoft SQL Server 2005**, auf **Konfigurationstools**, und klicken Sie anschließend auf **SQL Server-Oberflächenkonfiguration**.
2. Klicken Sie auf der Seite **SQL Server 2005-Oberflächenkonfiguration** auf **Oberflächenkonfiguration für Dienste und Verbindungen**.
3. Klicken Sie auf der Seite **Oberflächenkonfiguration für Dienste und Verbindungen** auf **SQL Server-Browser**, auf **Automatisch** als **Starttyp** und anschließend auf **Übernehmen**.

Hinweis: Wenn Sie auf die Option **Automatisch** klicken, wird der SQL Server-Browser-Dienst jedes Mal automatisch gestartet, wenn Sie Microsoft Windows starten.

4. Klicken Sie auf **Start** und anschließend auf **OK**.

Hinweis: Wenn Sie den SQL Server-Browser-Dienst auf einem Computer ausführen, zeigt der Computer die Instanznamen und Verbindungsinformationen zu allen Instanzen von SQL Server an, die auf dem Computer ausgeführt werden. Das Risiko kann verringert werden, indem man den SQL Server-Browser-Dienst nicht aktiviert und direkt über einen zugeordneten TCP-Port eine Verbindung zur Instanz von SQL Server herstellt. Die Herstellung einer direkten Verbindung zu einer Instanz von SQL Server über einen TCP-Port kann im Rahmen dieses Artikels nicht behandelt werden. Weitere Informationen zum SQL Server-Browser-Dienst und der Herstellung einer Verbindung zu einer Instanz von SQL Server finden Sie unter folgenden Themen in SQL Server-Onlinedokumentation:

- SQL Server-Browser-Dienst
- Herstellung einer Verbindung zum SQL Server-Datenbankmodul
- Client-Netzwerkkonfiguration
-

Ausnahmen in der Windows-Firewall erstellen

Diese Schritte gelten für die Version der Windows-Firewall, die in Windows XP Service Pack 2 (SP2) und in Windows Server 2003 enthalten ist. Wenn Sie ein anderes Firewallsystem verwenden, konsultieren Sie die entsprechende Firewalldokumentation.

Wenn Sie eine Firewall auf einem Computer mit SQL Server 2005 einsetzen, werden externe Verbindungen zu SQL Server 2005 blockiert, es sei denn, SQL Server 2005 und der SQL Server-Browser-Dienst können über die Firewall kommunizieren. Sie müssen eine Ausnahme für jede Instanz von SQL Server 2005 erstellen, die Remoteverbindungen annehmen soll, außerdem eine Ausnahme für den SQL Server-Browser-Dienst.

SQL Server 2005 verwendet eine Instanz-ID als Bestandteil des Pfades, wenn Sie die Programmdateien installieren. Sie müssen die richtige Instanz-ID ermitteln, um Ausnahmen für die einzelnen Instanzen von SQL Server zu erstellen. Gehen Sie folgendermaßen vor, um eine Instanz-ID zu ermitteln:

1. Klicken Sie auf **Start**, zeigen Sie auf **Programme**, auf **Microsoft SQL Server 2005**, auf **Konfigurationstools**, und klicken Sie anschließend auf **SQL Server-Konfigurations-Manager**.
2. Klicken Sie im SQL Server-Konfigurations-Manager im rechten Fensterbereich auf den SQL Server-Browser-Dienst, klicken Sie mit der rechten Maustaste auf den Instanznamen im Hauptfenster, und klicken Sie anschließend auf **Eigenschaften**.
3. Klicken Sie auf der Seite **Eigenschaften von SQL Server-Browser** auf die Registerkarte **Erweitert**, suchen Sie die Instanz-ID in der Eigenschaftenliste, und klicken Sie auf **OK**.

Um die Windows-Firewall zu öffnen, klicken Sie auf **Start**, auf **Ausführen**, geben Sie **firewall.cpl** ein, und klicken Sie anschließend auf **OK**.

Ausnahme für SQL Server 2005 in der Windows-Firewall erstellen

Gehen Sie folgendermaßen vor, um eine Ausnahme für SQL Server 2005 in der Windows-Firewall zu erstellen:

1. Klicken Sie in der Windows-Firewall auf die Registerkarte **Ausnahmen** und anschließend auf **Programm**.
2. Klicken Sie im Fenster **Programm hinzufügen** auf **Durchsuchen**.
3. Klicken Sie auf das ausführbare Programm "C:\Programme\Microsoft SQL Server\MSSQL.1\MSSQL\Binn\sqlservr.exe", klicken Sie auf **Öffnen** und

anschließend auf **OK**.

Hinweis: Der Pfad kann abhängig vom Installationsort von SQL Server 2005 anders aussehen. *MSSQL.1* ist ein Platzhalter für die Instanz-ID, die Sie in Schritt 3 der vorhergehenden Prozedur ermittelt haben.

4. Wiederholen Sie die Schritte 1 bis 3 für jede Instanz von SQL Server 2005, die eine Ausnahme erfordert.

Ausnahme für den SQL Server-Browser-Dienst in der Windows-Firewall erstellen

Gehen Sie folgendermaßen vor, um eine Ausnahme für den SQL Server-Browser-Dienst in der Windows-Firewall zu erstellen:

1. Klicken Sie in der Windows-Firewall auf die Registerkarte **Ausnahmen** und anschließend auf **Programm**.
2. Klicken Sie im Fenster **Programm hinzufügen** auf **Durchsuchen**.
3. Klicken Sie auf das ausführbare Programm "C:\Programme\Microsoft SQL Server\90\Shared\sqlbrowser.exe", klicken Sie auf **Öffnen** und anschließend auf **OK**.

Hinweis: Der Pfad kann abhängig vom Installationsort von SQL Server 2005 anders aussehen.